



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

50

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/646,640	11/09/2000	Patrick Salle	00621/TL	1842
41754	7590	03/18/2005	EXAMINER	
PEHR JANSSON, ATTORNEY AT LAW 7628 PARKVIEW CIRCLE AUSTIN, TX 78731			KIM, JUNG W	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 03/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/646,640

Applicant(s)

SALLE, PATRICK

Examiner

Jung W Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 14 December 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 2-13 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 2-13 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 December 2004 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 12/2004.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. Claims 2-13 have been examined. Applicant in the amendment filed on December 14, 2004 amended claims 2-8, added new claims 9-13 and canceled claim 1.

#### ***Response to Amendment***

2. The objection to the title is withdrawn as the amended title more clearly indicative of the claimed invention.
3. The 112, 2<sup>nd</sup> paragraph rejection to claim 1 is withdrawn as the claim has been canceled.

#### ***Response to Arguments***

4. Applicant's arguments filed December 14, 2004 have been fully considered but they are not persuasive.

5. On pg. 9 2<sup>nd</sup> full paragraph, applicant argues:

*Kocher fails to disclose a method for protecting data element from discovery by analysis of the microprocessor's electric power consumption because Kocher refers only to timing attacks (and not power attacks), which timing attacks measure time delays between data input times and data output times for several different input data.*

6. In response to applicant's arguments, the recitation "from discovery by analysis of the microprocessor's electric power consumption" has not been given patentable

weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951). See also MPEP 2111.02 and 2112 (I).

7. Applicant further argues:

*In addition, Kocher fails to disclose the random transformation of at least one of the data elements by associating said at least one of the data elements with a random number generated by associating the at least one of the data elements with a random number generated by an unpredictable number generator, by means of a logical operator of the exclusive-OR type. The use of a signature scheme proposed by Kocher is different from the invention recited in Claim 9... (pg. 9, 3<sup>rd</sup> full paragraph).*

8. In reply, applicant argues against the references individually (Kocher teaches blinding operations to disguise the type and order of operations of a cryptographic method, see Kocher, Abstract, pg. 1, section 1; pgs. 8-9, section 10; Schneier teaches the random transformation of at least one of the data elements by associating said at least one of the data elements with a random number generated by associating the at least one of the data elements with a random number generated by an unpredictable number generator, by means of a logical operator of the exclusive-OR type; see

Art Unit: 2132

Schneier, pg. 295, "DSX" and section 15.6 'Whitening'), as such, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

### ***Drawings***

9. The drawings were received on December 14, 2004. These drawings are not acceptable since they contain new matter. (see section titled "Specification" in the instant office action) It is suggested that revised drawings depicting only the illustrative differences between alternative embodiments (flow charts wherein a randomly transformed data element is a message block, wherein the randomly transformed data element is a message block associated with a key by logical operator of the exclusive-OR type, and wherein the random transformation step is a step that precedes the group of operations executed repeatedly and in which the inverse transformation step follow the group of repeated operations) be submitted to overcome the objections to the drawings as outlined below.

10. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the limitations of: 1) the randomly transformed data element being a message block (M, M0, M1, M2, M3) (claim 3), 2) the randomly transformed data element being a message block associated with a key by a logical operator of the exclusive-OR type (claim 4), and 3) a random

transformation step preceding the group of operations (270) and the inverse random transformation step following the group of operations (270) (claim 6) must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

11. Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### ***Specification***

12. The amendment filed December 14, 2004 is objected to under 35 U.S.C. 132 because it introduces new matter into the disclosure. 35 U.S.C. 132 states that no amendment shall introduce new matter into the disclosure of the invention. The added

Art Unit: 2132

material which is not supported by the original disclosure is as follows: Figure 2 defines a random transformation of bits of the message M3 to M3\* after step 30 and before step 210 (in this instance, the specification only defines an alternative embodiment wherein the randomly transformed data element is a message block, but does not disclose all of material of Figure 2-also, the figure is problematic because M3\* is never referred to again in the flow diagram); Figure 3 defines a random transform between step 210 and 220 (in this instance, the specification only defines an alternative embodiment wherein the randomly transformed data element is a message block associated with a key by logical operator of the exclusive-OR type, but does not disclose all of Figure 3-also, it is not clear what the random transform does in this particular instance); Figure 4 defines step 270 to incorporate exactly steps 30, 130, 140 and 210; (in this instance, the specification only defines an alternative embodiment wherein the random transformation step precedes the group of operations executed repeatedly and in which the inverse transformation step follow the group of repeated operations, but does not disclose all of Figure 4).

13. Applicant is required to cancel the new matter in the reply to this Office Action.

### ***Claim Objections***

14. Claim 9 is objected to because of the following informalities: in claim 9, line 7 the word "least" is misspelled. Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

15. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

16. Claims 2-7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

17. Claims 2-7 recites the limitations "(K1,K2,K3,K4,K5)", "(M,M0,M1,M2,M3)", "(R1,R2,R3,R4,R5)" and "(270)", however, it is not clear as to whether the feature introduced by such language is (a) merely exemplary of the remainder of the claim, and therefore not required, or (b) a required feature of the claims. The cancellation of claim 1 rendered these limitations indefinite.

***Claim Rejections - 35 USC § 103***

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

19. Claims 2-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier Applied Cryptography 2<sup>nd</sup> Edition (hereinafter Schneier) in view of Kocher "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems" (hereinafter Kocher).



20. As per claim 9, Schneier discloses a data protection method using a cryptographic algorithm for executing operations for processing data elements so as to generate encrypted information (see Schneier, pgs. 265-301, DES), the method comprising: random transform of at least one of the data elements by associating the at least one of the data elements with a random number generated by an unpredictable number generator, by means of a logical operator of the exclusive-OR type, and after this random transformation step, an inverse transformation step such that the encrypted information is unchanged by these transformation steps. See Schneier, page 295, 'DESX'; pages 366-367, section 15.6 'Whitening'. Further, it notoriously well known in the art for DES or DES type encryption to be processed by a microprocessor in a chip card, since DES was the standard means of efficiently encrypting messages submitted to or from a user. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the method to be contained in a microprocessor of a chip card since a chip card enables portable but cryptographically secure transaction means as known to one of ordinary skill in the art. See also Schneier, pg. 587, section 24.13, 'Smart Cards'.

21. Finally, Schneier does not expressly disclose incorporating the data protecting method to protect data elements from discovery by analysis of the microprocessor's electric power consumption. Kocher teaches a method of using a blinding factor to mask a data element in a cryptographic method, wherein the blinding factor prevents an attacker from observing these data values used in a cryptographic step of this method;

(timing attacks observe the different amounts of time to process different inputs-this distinction also inherently includes different power fluctuations generated by the different amounts of time). A random transform is applied to a data element prior to input of an encryption step and an inverse random transform is applied to the output of the encryption step. This blinding factor leaves the ensuing ciphertext unchanged by the random transformation and its inverse step (see Kocher, page 8, 'Preventing the Attack'). Furthermore, although the random transformation example disclosed by Kocher is a blinding factor specifically using modular multiplication in a public key methodology, the teaching of a blinding factor generalizes to any cryptographic method whenever an attacker can observe a portion of the method (see Kocher, page 1, 'Introduction'; page 8, 3<sup>rd</sup> full paragraph, second sentence). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Kocher to the method taught by Schneier since it enables the method to prevent attacks based on measured observations of certain cryptographic operations of a cryptosystem as taught by Kocher, *ibid*. The aforementioned cover the limitations of claim 9.

22. As per claims 2-4, the rejection of claim 9 is incorporated herein. In addition, the subset of consecutive operations that are commutative in the DES cryptographic method, which allows such a random transformation and its inverse transformation without changing the encrypted information, enables the randomly transformed data element to be any of the following: a key (K1, K2, K3, K4, K5), a message block (M, M0, M1, M2, M3), and/or a message block associated with a key by a logical operator of the

exclusive-OR type (R1, R2, R3, R4, R5). Also, means of adjusting or shifting location of parts for the random transformed data element to be any of a key, a message block, and/or message block associated with a key by a logical operator of the exclusive-OR type is an obvious enhancement. See *In re Stevens* 101 USPQ 284 (CCPA 1954) and *In re Japikse* 86 USPQ 70 (CCPA 1950). The aforementioned cover the limitations of claims 2-4.

23. As per claim 5, the rejection of claim 9 is incorporated herein. In addition, the cryptographic algorithm for executing operations for processing data comprises a group of operations executed repeatedly. See Schneier, page 270, 3<sup>rd</sup> full paragraph.

24. As per claim 6, the rejection of claim 5 is incorporated herein. In addition, the random transformation step precedes the group of operations executed repeatedly and the inverse transformation step follows the group of operations (270). See Schneier, page 272, Figure 12.2; page 366, last paragraph, first sentence.

25. As per claim 8, the rejection of claims 9 is incorporated herein. In addition, the cryptographic algorithm is a DES type. See Schneier, pages 265-301, DES.

26. As per claims 7 and 10-13, the rejections of claims 2-4 are incorporated herein. Further, the step of randomly modifying the order of execution of operations from one cycle to another, a cycle being a complete execution cycle of the algorithm or an

intermediate cycle of a group of operations, the operations being operations whose order of execution relative to the others does not affect the result is a trivial attribute. DES is a series of cryptographic steps wherein a subset of the steps are not tied directly to a specific ordering of operations due to the mathematical nature of the method: the commutative property of many of the steps within a cycle trivially allows for reordering of operations without changing the resulting encrypted text; these orderings include permutation of bits of a message block before permutation of bits of a key, and vice versa, and modifying the order of processing quartets making up a data element; furthermore, it has been shown that adjusting and/or reordering of parts is an obvious enhancement. See *In re Stevens* 101 USPQ 284 (CCPA 1954) and *In re Japikse* 86 USPQ 70 (CCPA 1950). Finally, something that is old (randomly modifying order of execution of commutative operations) does not become patentable upon the discovery of a new property (cryptanalysis by observing fluctuating power consumption on the execution of operations). See MPEP 2112 (I). The aforementioned cover the limitations of claims 7 and 10-13.

### ***Conclusion***

27. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

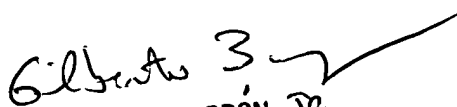
Application/Control Number: 09/646,640  
Art Unit: 2132

Page 13



Jung W Kim  
Examiner  
Art Unit 2132

Jk  
March 8, 2005



GILBERTO BARRÓN JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100